学校编码：10384　　分类号＿＿＿密级＿＿

学　　号：X2008230180　　UDC＿＿＿

硕　士　学　位　论　文

统一认证授权平台的设计与实现

Design and Implementation of theUnified authentication and authorization platform

赵　亮

指导教师姓名：杨双远副教授

专　业　名　称：软　件　工　程

论文提交日期：2010 年　　月

论文答辩时间：2010 年　　月

学位授予日期：2011 年　　月

答辩委员会主席：＿＿＿＿＿＿

评　　阅　　人：＿＿＿＿＿＿

2010 年　　月

厦门大学学位论文原创性声明

本人呈交的学位论文是本人在导师指导下,独立完成的研究成果。本人在论文写作中参考其他个人或集体已经发表的研究成果，均在文中以适当方式明确标明，并符合法律规范和《厦门大学研究生学术活动规范（试行）》。

另外，该学位论文为（　　）课题（组）的研究成果，获得（　　）课题（组）经费或实验室的资助，在（　　）实验室完成。（请在以上括号内填写课题或课题组负责人或实验室名称，未有此项声明内容的，可以不作特别声明。）

声明人（签名）：

年　　月　　日

厦门大学学位论文著作权使用声明

本人同意厦门大学根据《中华人民共和国学位条例暂行实施办法》等规定保留和使用此学位论文，并向主管部门或其指定机构送交学位论文（包括纸质版和电子版），允许学位论文进入厦门大学图书馆及其数据库被查阅、借阅。本人同意厦门大学将学位论文加入全国博士、硕士学位论文共建单位数据库进行检索，将学位论文的标题和摘要汇编出版，采用影印、缩印或者其它方式合理复制学位论文。

本学位论文属于：

（　　）1.经厦门大学保密委员会审查核定的保密学位论文，于　　年　　月　　日解密，解密后适用上述授权。

（　√　）2.不保密，适用上述授权。

（请在以上相应括号内打“ √”或填上相应内容。保密学位论文应是已经厦门大学保密委员会审定过的学位论文，未经厦门大学保密委员会审定的学位论文均为公开学位论文。此声明栏不填写的，默认为公开学位论文，均适用上述授权。）

声明人（签名）：

年　　月　　日

摘 要

信息系统在进行信息交互时，首先需要鉴别访问主体的身份（防止主体身份被伪造），并保证在访问客体时是以主体的真实身份进行正确的访问，因此，认证和授权是信息安全的第一关。在企业信息安全体系中扮演着重要的角色，如果认证授权机制安全强度较弱，非法用户能够较容易的方式、方法冒用合法用户的身份访问信息系统，即使信息系统访问控制、加密等安全防范措施再完善，也不能防范非法用户访问信息系统，极大的威胁信息系统的安全，因此认证和授权对于保障信息系统安全非常重要。认证和授权不仅是一个单独的安全机制，其涵盖的内容还包括用户身份信息集成、用户单点登录等内容，也是企业应用集成的基础和重要内容。

本文通过对认证、授权、访问控制业务的详细分析，结合本企业内部的具体要求，首先分析了统一认证授权平台的功能需求；其次，对平台的各功能模块进行了划分，详细分析了各子系统的具体功能，在此基础上给出了总体设计方案和数据库设计方案以及业务模型设计方案。最后，介绍了平台的具体实施及实现效果。

本文以软件工程的思想为主线，从需求分析、框架设计、功能模块设计、数据库设计、系统实现和集成测试等方面介绍了系统的实施过程。

关键词：身份认证；访问控制；业务模型设计；UAAP

Abstract

Information systems to interacting,the first is user idengtification (to prevent the identify was forged), and to assure real identity who is accessing the object and going on proper access, so authentication and authorization is primary to information security, it plays an important role in information security system of enterprises. If the strength of security about authentication and authorization is weak, illegal users can masqueade as legal users to access the information system by easy manner and method. Even if the access control and encryption of information systems is improving, it can't prevent illegal access, and that is a great threat to security of information systems. Authentication and authorization for the protection information system security is very important. Authentication and authorization is not only a single security mechanism, they covers information integreation of users and SSO(single sign-on) of user etc, and it is the base and important content of EAI.

In this paper, a unified authentication and authorization platform is developed in this context, this article through authentication, authorization, access control, detailed analysis of the business, combined with the specific requirements of the enterprise, first proposed a unified authentication and authorization platform functional requirements; secondly, on the platform by the various function modules, detailed analysis of the specific functions of the subsystems, on this basis, given the overall design and database design and business model design. Finally, the concrete implementation of the platform and achieve results.

In this paper, the main line of software engineering, from requirements analysis, framework design, module design, database design, system implementation and integration testing, introduces the system implementation process.

Keywords: Authentication; access control; business model design; uaap

目 录

第一章 绪 论 ……1

1.1 课题背景及建设意义 ……1
1.2 国内外研究现状 ……3
1.3 主要研究内容及特色 ……3
1.4 论文组织结构 ……4

第二章 统一认证授权平台的需求分析 ……5

2.1 平台的架构需求 ……5
2.2 功能需求 ……6
2.2.1 高级用例 ……6
2.2.2 UAAP 功能 ……7
2.2.3 管理台 ……9
2.2.4 认证及 SSO ……10
2.2.5 访问控制 ……10
2.2.6 信息发布及数据同步 ……11
2.2.7 网络设备及操作系统接入 ……12
2.3 性能需求 ……13
2.4 本章小结 ……13

第三章 统一认证授权平台的设计及实现 ……14

3.1 应用架构设计 ……14
3.2 总体架构 ……15
3.3 功能设计 ……17
3.3.1 数据存储子系统 ……17
3.3.2 数据同步子系统 ……19
3.3.3 认证服务子系统 ……20
3.3.4 访问控制服务子系统 ……21
3.3.5 管理台子系统 ……21
3.4 数据库设计 ……23
3.4.1 关系型数据库设计 ……23
3.4.2 LDAP Schema 设计 ……26
3.5 统一身份认证与授权模型设计 ……42
3.5.1 身份信息模型 ……43
3.5.2 认证信息模型 ……45
3.5.3 角色权限模型 ……46
3.5.4 数据权限模型 ……46
3.6 关键代码实现 ……47
3.6.1 公共函数 ……47
3.6.2 交易分发服务 ……51
3.6.3 静态口令的提示信息校验－1001 ……53

3.6.4 静态口令校验－1002 ……53
3.6.5 设置静态口令提示信息－1003 ……53
3.6.6 生成静态口令－1004 ……54
3.7 本章小结 ……55
第四章　认证授权平台的实施 ……56
4.1 部署情况 ……56
4.2 工作原理 ……57
4.3 系统性能 ……59
4.3.1 性能测试硬件一览表 ……59
4.3.2 环境配置 ……60
4.3.3 环境资源初始 ……61
4.3.4 环境部署图 ……62
4.3.5 生产系统处理能力估算 ……62
4.4 本章小结 ……63
第五章　总结与展望 ……64
5.1 总结 ……64
5.2 展望 ……64
参考文献 ……66
致　谢 ……68

CONTENTS

CHAPTER1 INTRODUCTION ……1

1.1 BACKGROUND AND SIGNIFICANCE OF TOPIC ……1
1.2 RESEARCH STATUS ……3
1.3 MAIN CONTENTS AND CHARACTERISTICS ……3
1.4 PAPER ORGANIZATION ……4

CHAPTER2 UNIFIED AUTHENTICATION AND AUTHORIZATION PLATFORM NEEDS ANALYSIS ……5

2.1 PLATFORM ARCHITECTURE NEEDS ……5
2.2 FUNCTIONAL REQUIREMENTS ……6
2.2.1 Advanced use cases ……6
2.2.2 UAAP function ……7
2.2.3 Management units ……9
2.2.4 Authentication and SSO ……10
2.2.5 Access Control ……10
2.2.6 Information distribution and data synchronization ……11
2.2.7 Access network equipment and operating systems ……12
2.3 PERFORMANCE REQUIREMENTS ……13
2.4 CHAPTER SUMMARY ……13

CHAPTER3 UNIFIED AUTHENTICATION AND AUTHORIZATION PLATFORM FOR THE DESIGN AND IMPLEMENTATION ……14

3.1 APPLICATION ARCHITECTURE DESIGN ……14
3.2 GENERAL FRAMEWORK ……15
3.3 FUNCTIONAL DESIGN ……17
3.3.1 Data storage subsystem ……17
3.3.2 Data synchronization subsystem ……19
3.3.3 Certification service subsystem ……20
3.3.4 Access control service subsystem ……21
3.3.5 Management station subsystem ……21
3.4 DATABASE DESIGN ……23
3.4.1 Relational Database Design ……23
3.4.2 LDAP Schema Design ……26
3.5 UNIFIED AUTHENTICATION AND AUTHORIZATION MODEL DESIGN ……42
3.5.1 Identity model ……43
3.5.2 Certification Information Model ……45
3.5.3 Role permissions model ……46
3.5.4 Data permissions model ……46
3.6 KEY CODE ……47
3.6.1 Public Functions ……47
3.6.2 Trading Distribution Service ……51
3.6.3 Check static password prompt－1001 ……53
3.6.4 Static password check－1002 ……53
3.6.5 Set the static password prompt－1003 ……53
3.6.6 Generate static password－1004 ……54

3.7 CHAPTER SUMMARY ·····55
CHAPTER4 THE IMPLEMENTATION OF AUTHENTICATION AND AUTHORIZATION PLATFORM ·····56
4.1 DEPLOYMENT ·····56
4.2 WORK ·····57
4.3 SYSTEM PERFORMANCE ·····59
4.3.1 List of Performance Test Hardware ·····59
4.3.2 Environment configuration ·····60
4.3.3 The initial environmental resources ·····61
4.3.4 Environmental deployment diagram ·····62
4.3.5 Estimation of the production system capacity ·····62
4.4 CHAPTER SUMMARY ·····63
CHAPTER5 CONDITIONS ·····64
5.1 SUMMARY ·····64
5.2 OUTLOOK ·····64
REFERENCES ·····66
THANK ·····68

第一章　绪　论

随着企业各项业务向电子化、数字化、网络化的发展，对信息系统的重视和依赖程度越来越高，各种信息技术高新技术尤其是网络应用的发展，进一步提高了企业计算机的应用广度及水平。在享受这些新型产品带来便利和效率的同时，我们也深刻感受到计算机网络应用安全及其管理问题的日益突出及其所带来的金融风险。本章将统一认证授权平台为例，阐述一种解决方案，并对本文研究内容以及本文的结构安排进行总体概述。

1.1 课题背景及建设意义

进入 21 世纪，经济全球化和我国改革开放事业的发展，对我国银行业的发展带来巨大的冲击——国内商业银行的组织架构、业务流程、管理体制、营销体系等多个方面都需要“以变应变”，转型成为我国银行业发展的主旋律。

在这样的变革时期，如何保证银行企业的核心竞争力？在目前经济和行业背景下，有效提升银行竞争力有多种方式，加强风险管理和金融创新是其中最主要的两种途径。

信息系统统一认证和授权平台（UAAP）建设正是在这样的背景下启动的。统一认证与授权平台是整体 IT 架构中的基础设施。通过建立统一的、与业务流程无关的用户身份信息管理、统一的身份认证与统一授权机制为国内商业银行的整体风险控制和管理、金融业务的创新提供重要支持和保障。

“所谓银行就是基于风险处理能力而盈利的组织”[1]。本质上风险管理能力就是银行的核心能力。为了适应金融全球化趋势、金融风险管理技术的迅速发展，强化金融风险管理的新《巴塞尔资本协议》应运而生。巴赛尔协议是防范金融风险的，“新巴赛尔协议在信贷、营运风险要求的基础上，增加了防范操作风险的要求”[2]。如何有效地利用信息化来为金融行业的风险监控提供支持是近年来银行业的一个热点话题。在降低操作风险的内容中，可以从建立信息安全保障体系着手来降低业务营运风险，支持巴赛尔协议。UAAP 的建立为全面支持巴塞尔协议提供了信息技术保障，具有极其重要的意义。

此外，目前银行业基本完成了数据大集中的工作。数据集中后，如何高效地管理和利用金融系统庞大的、分散的、冗余的客户信息，是银行业信息主管部门所面临的最迫切问题。银行业需要与之相适应的安全和管理体系，强化运营管理和安全管理，保障银行业务处理系统的平稳运行。

在银行信息安全保障方面人民银行出了一个指导意见——《中国人民银行关于进一步加强银行业金融机构信息安全保障工作的指导意见》。UAAP 的建设是贯彻落实《指导意见》内容要求的必要条件。

银行业也需要根据自己实际业务需要提出了建立信息安全保障体系，从管理、运营、服务上建立完善的安全保障措施。如图 1.1 所示：

图 1.1 企业安全保障体系

这其中的用户管理、身份认证和授权及其相关配套的运营、管理等部分内容可以由 UAAP 来完成。

总之，UAAP 平台的建设是解决数据大集中与信息安全的矛盾的内在要求，也是银行对外遵循《新巴塞尔协议》、《萨班斯法》[3]等国际法案的具体行动和体现。

平台不仅在技术上为其它系统提供统一的安全服务，防范操作风险，而且通

过提供统一的用户身份管理，统一认证和授权机制，逐步实现信息系统用户身份信息的整合，实现面向用户的认证和授权服务，为企业的业务创新提供有力保障。

从信息化本身的创新能力来说，为了提高开发效率，减少系统维护成本，有必要打破早期信息化建设各系统自成一体的局面，按照组件化、标准化、安全、可扩展四原则建立新的 IT 技术架构，实现企业系统本身的创新。平台将建立各应用系统统一的用户管理机制，统一的授权和认证机制，不仅提高了各应用系统的安全等级，而且使业务系统开发时只须专注核心业务逻辑的开发，提高了代码复用的程度，降低了开发和维护成本，使得整体 IT 技术架构层次更加清晰合理。

1.2 国内外研究现状

上海交通大学汪良生以上海交通银行的应用需求和安全需求为背景，提供了一个商业银行统一认证方案，为银行传统业务系统和网络应用服务提供了一个统一的安全认证平台。该方案采用 IBM 数据联邦技术，实现了用户身份信息及安全策略的整合，避免了数据迁移。运用 SAML（安全声明标记语言）技术，作为认证授权结果的标准化表示和传递，解决了各业务系统间的安全信息共享。运用单点登录技术提供统一认证和集中授权服务，并加入集中管理和审计功能，实现了增强 4A 型（认证、授权、管理、审计）安全服务。

本平台通过对企业内不同信息系统安全服务的整合，建立了企业范围内的统一身份管理、身份认证、访问控制平台。提供了不同强度的安全机制，支持静态口令、动态口令、数字证书、生物特征（指纹）等多种认证方式。扩充了 RBAC 标准，增加了全局角色和应用角色，通过身份管理服务、认证服务、授权服务、访问控制服务和单点登录服务组合出 6 种服务模式。

1.3 主要研究内容及特色

通过对各应用系统的身份信息及权限要素的分析，建立起统一认证授权的业务模型，对各应用系统中的用户身份信息进行统一的认证和授权管理，建立统一用户视图，实现用户身份信息的统一存储。

在用户身份信息集中统一的基础上，为不同应用系统提供认证服务。

建立统一的授权管理规则，实现对访问者、资源和访问控制规则的统一描述，

实现基于角色的访问控制，为用户方位多应用实现单点登录。

建立中心和分布用户存储，实现关键业务和管理应用系统信息的同步，建立用户信息的分权管理机制。

对于真正的用户，其特色主要体现在：

- 用户只需要记住一个口令，当口令快到期时候，系统会有提醒功能，用户也只需要修改一个口令。
- 新员工上岗，只需要确定其岗位做一次授权工作后便可具有其岗位所能操作的所有应用系统的权限。

对于接入系统来说，其特色体现在：

- 只要接入平台，无需开发认证与访问控制、授权等功能。
- 平台可以提供多种服务自行选择复杂的认证策略可以适用于所有应用系统，无需系统自行开发。

对于企业来说，其特色体现在：一夫当关，万夫莫开。如果某一个员工被辞退，只需在平台内做一次用户状态修改，此人就无法进入所有系统。

1.4 论文组织结构

本论文重点探讨“统一认证授权平台”的需求分析、总体设计与实现、实施及应用界面展示、总结与展望等，介绍技术难点，分析论题要点。

总共分为五章，组织结构如下：

第一章介绍了大型企业建立“统一认证授权平台”的背景、目的、内容以及研究的意义。

第二章介绍平台的需求分析。描述需求，描述业务要素及之间的关系。

第三章探讨“统一认证授权平台”的设计与实现。介绍平台的架构设计、功能子系统的划分和核心数据库表的表结构、LDAP 结构以及部分代码。

第四章研究如何实施平台。介绍平台的部署情况和工作原理以及性能测试。

第五章总结了平台实现的主要功能及展望，剖析“统一认证授权平台”中的技术创新、独特的软件视角等等。展望了未来平台的拓展空间，以便更好地为企业各业务系统提供服务。

第二章　统一认证授权平台的需求分析

在本章中，我们将对统一认证授权平台的需求进行介绍，并对需求和功能进行详细解释，使读者对论文研究基础有所了解。

2.1 平台的架构需求

UAAP 作为一个基础的服务，为其它应用系统提供统一身份管理和访问控制服务，采用总行集中、分行分布式部署的方式，如图 2.1 所示。

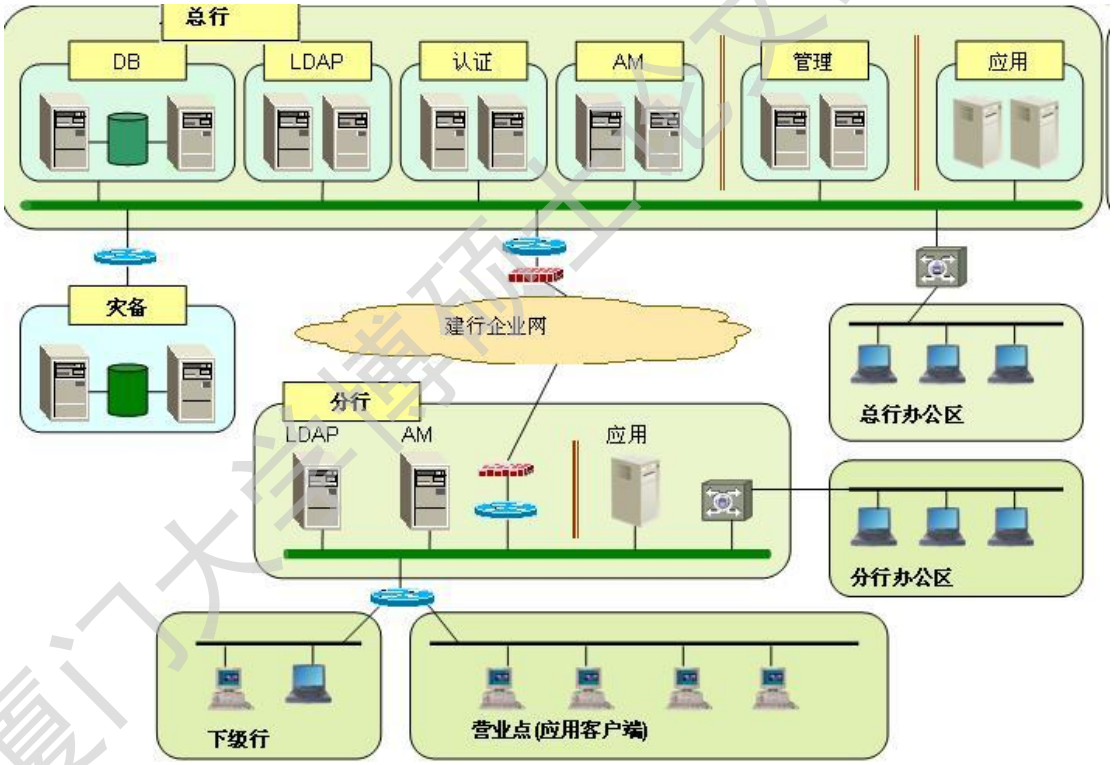

图 2.1 物理架构

在数据层，系统使用集中统一的数据源，为 DB。

在管理层，使用统一的管理控制台，并对数据源进行实时的同步更新；

在服务和应用运行层，每个应用可以部署独立的认证、策略服务器，或者和其它应用共享这些服务器，根据应用的需求来定。

为有效的分流对 AM（访问管理服务）的访问请求和对 LDAP 的访问请求，

在适应总行部署的前提下，分行部署了独立的 AM（访问管理服务）服务器和 LDAP 目录服务器，通过 IDM 实现总分行信息的发布，有效地分流接入应用对总行 AM（访问管理服务）和 LDAP 的访问请求减轻访问压力，同时提高了分行应用的可用性。

总行集中部署的应用直接与总行 UAAP 接入，总分行推广以及分行特色的应用则根据应用部署地域的不同分别接入相应的 UAAP 总行或分行 AM（访问管理服务）、LDAP。UAAP 管理层面统一使用 UAAP 总行管理台进行管理。

2.2 功能需求

2.2.1 高级用例

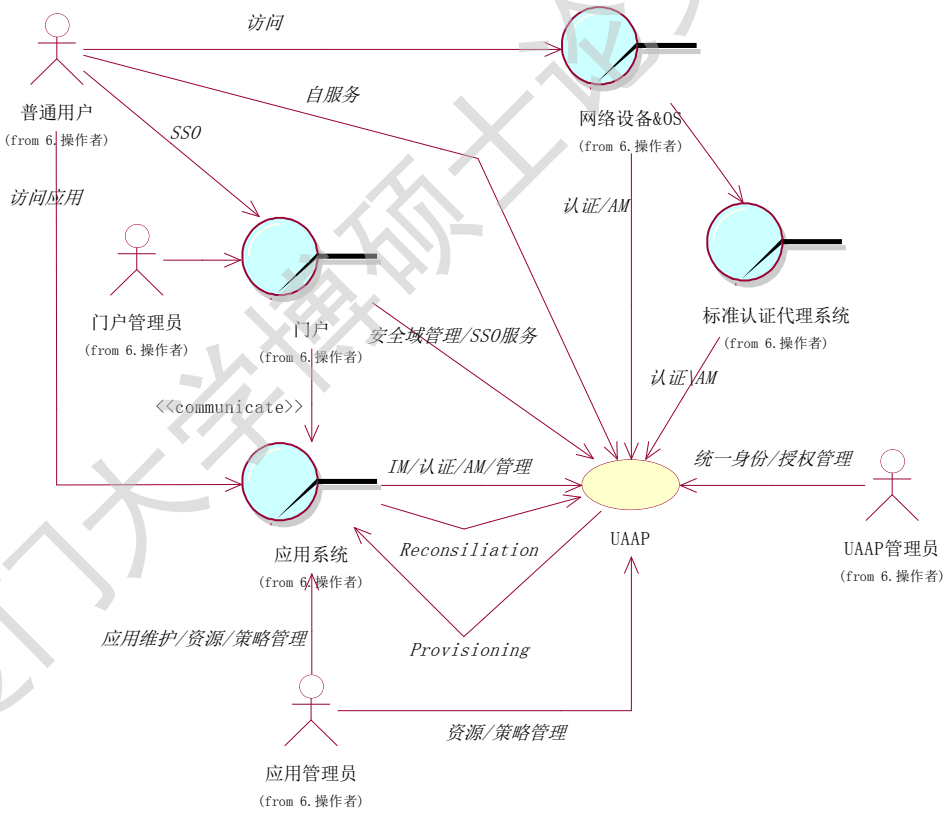

图 2.2 高级用例

图 2.2 描述了 UAAP 作为一个平台，和外部各种设施和人员之间的交互关系，所有这些交互构成了 UAAP 平台的功能性需求。

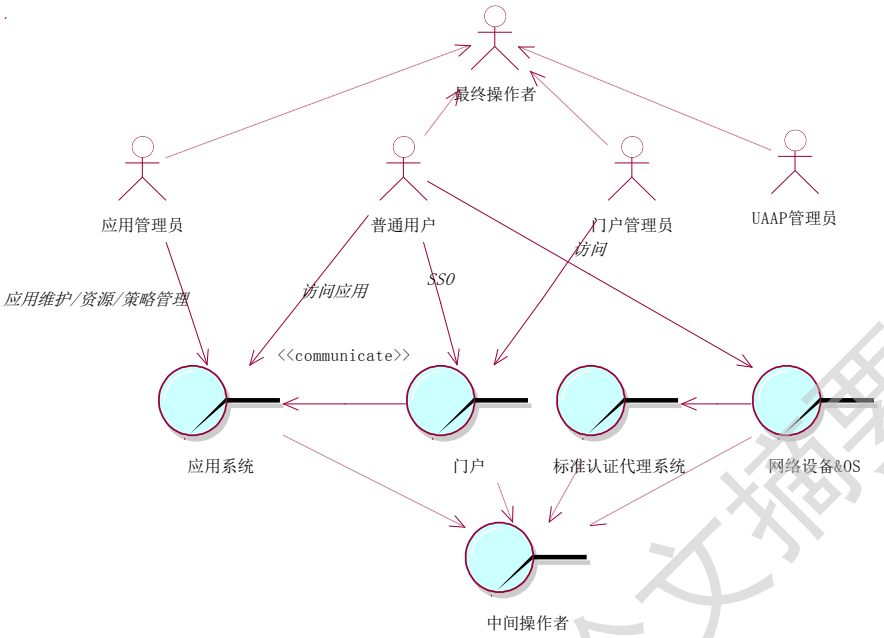

图 2.3 操作者分类

操作者的分类：分为最终操作者和中间操作者；由最终操作者引发界面需求和界面设计；由中间操作者引发接口设计。

2.2.2 UAAP 功能

信息发布/数据同步子系统，由项目组基于产品开发实现，完成 DB→LDAP 和 LDAP→应用之间的数据同步功能；认证服务子系统，在一期认证服务的基础上扩展改造；访问控制服务子系统，由 SiteMinder 实现；管理台子系统，由项目组开发实现，完成身份、认证、授权等管理相关的各种功能；应用接入和平台接口，是平台提供给应用系统调用的管理、认证和访问控制的接口和代理，主要包括：管理接口、一期认证接口和二期基于 SiteMinder 的认证、访问控制和 SSO 应用开发接口及代理模块。如图 2.4 所示。